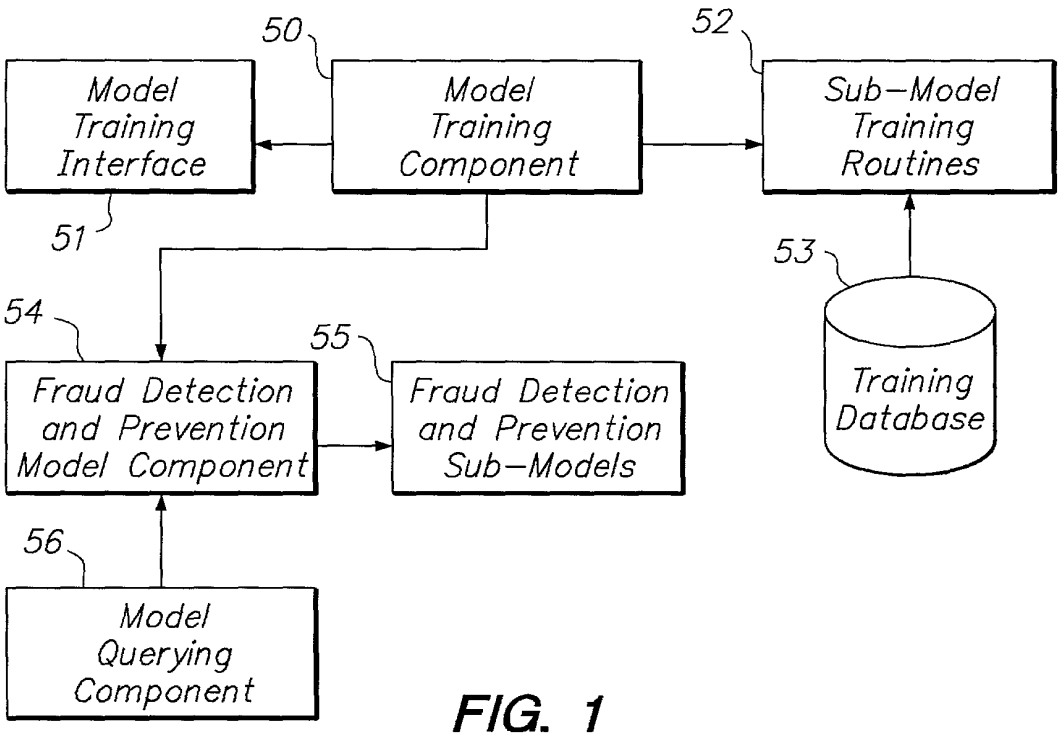


FIG. 1

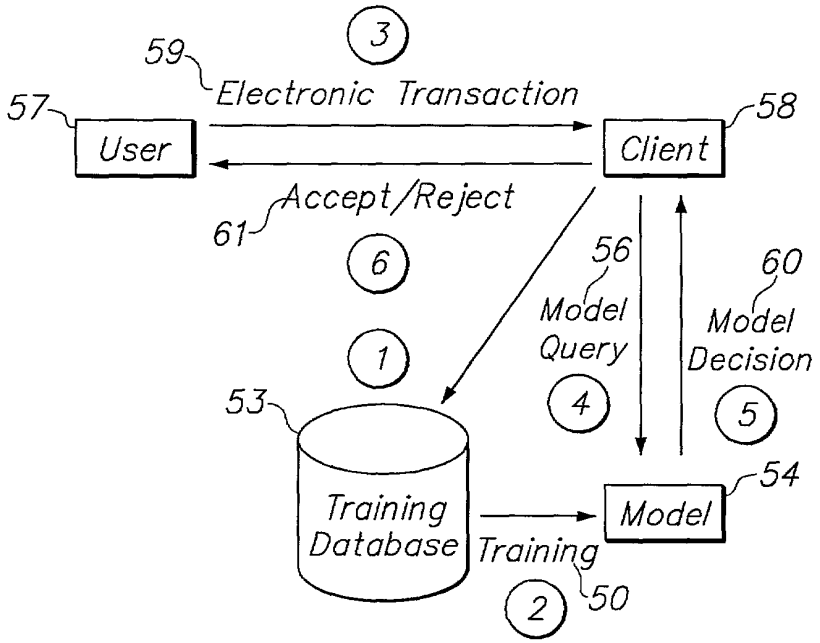


FIG. 2

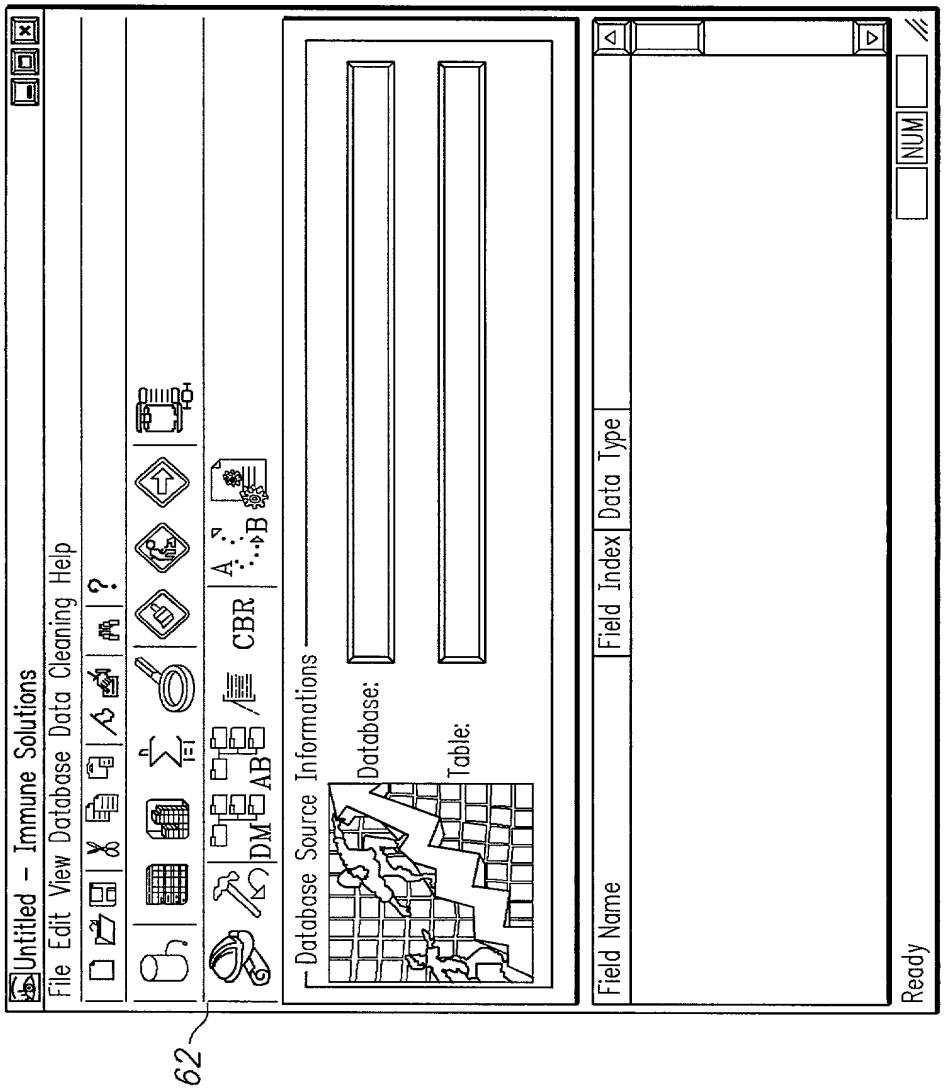

Untitled - Immune Solutions
File Edit View Database Data Cleaning Help
DM
AB
CBR
Database Source Informations
Database:
Table:
Field Name
Field Index
Data Type
NUM
Ready
62

FIG. 3

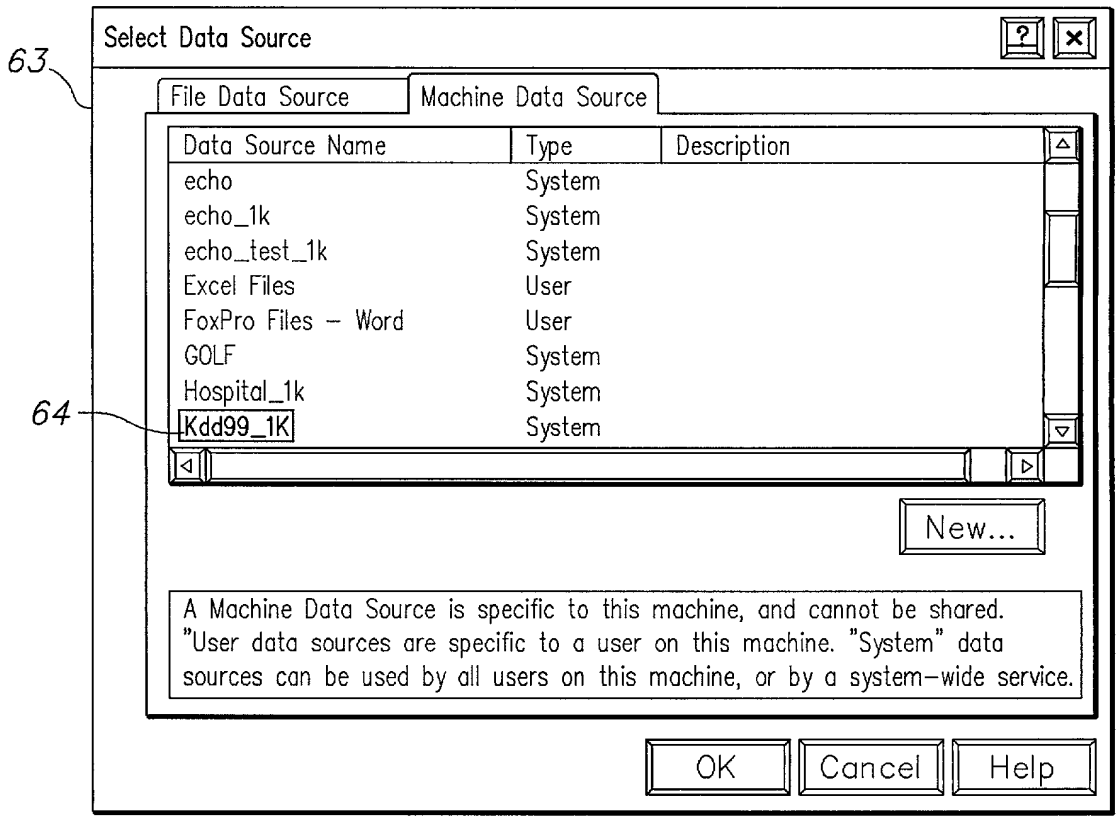

Select Data Source
63
File Data Source
Machine Data Source
Data Source Name
Type
Description
echo
System
echo_1k
System
echo_test_1k
System
Excel Files
User
FoxPro Files – Word
User
GOLF
System
Hospital_1k
System
64
Kdd99_1K
System
New...
A Machine Data Source is specific to this machine, and cannot be shared. "User data sources are specific to a user on this machine. "System" data sources can be used by all users on this machine, or by a system-wide service.
OK
Cancel
Help

FIG. 4

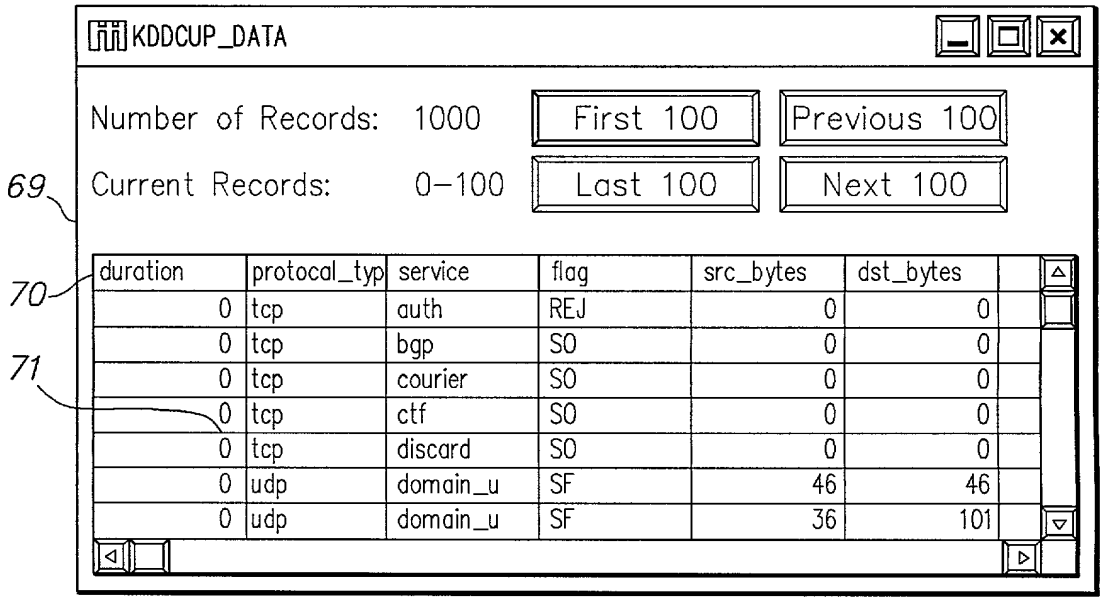

KDDCUP_DATA
Number of Records: 1000
First 100
Previous 100
69
Current Records: 0–100
Last 100
Next 100
70
71
duration
protocal_typ
service
flag
src_bytes
dst_bytes
0 tcp auth REJ 0 0
0 tcp bgp SO 0 0
0 tcp courier SO 0 0
0 tcp ctf SO 0 0
0 tcp discard SO 0 0
0 udp domain_u SF 46 46
0 udp domain_u SF 36 101

FIG. 6

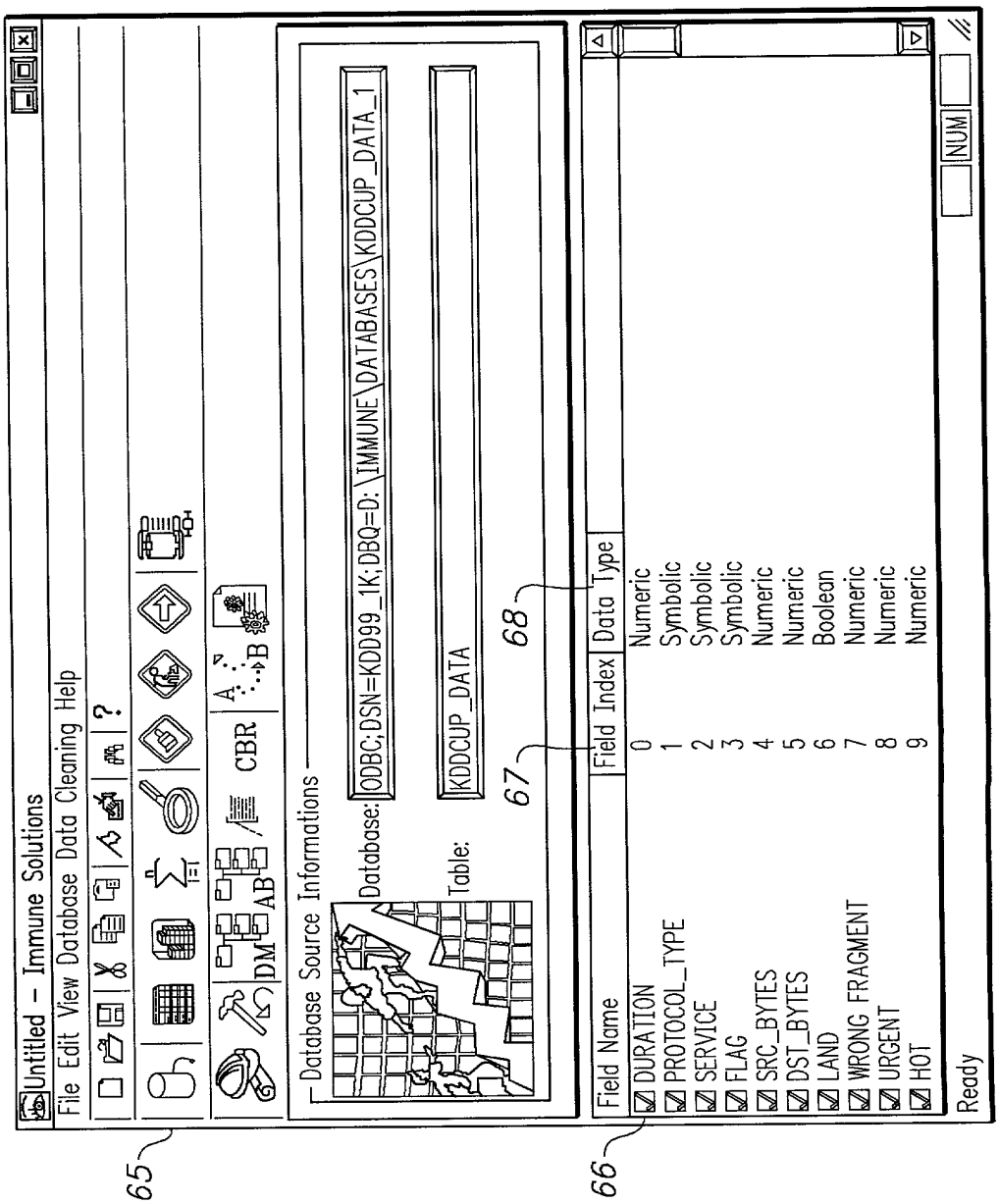

Untitled – Immune Solutions
File Edit View Database Data Cleaning Help
CBR
Database Source Informations
Database:
ODBC;DSN=KDD99_1K;DBQ=D:\IMMUNE\DATABASES\KDDCUP_DATA_1
Table:
KDDCUP_DATA
65
66
67
68
Field Name
Field Index
Data Type
DURATION 0 Numeric
PROTOCOL_TYPE 1 Symbolic
SERVICE 2 Symbolic
FLAG 3 Symbolic
SRC_BYTES 4 Numeric
DST_BYTES 5 Numeric
LAND 6 Boolean
WRONG FRAGMENT 7 Numeric
URGENT 8 Numeric
HOT 9 Numeric
Ready
NUM

FIG. 5

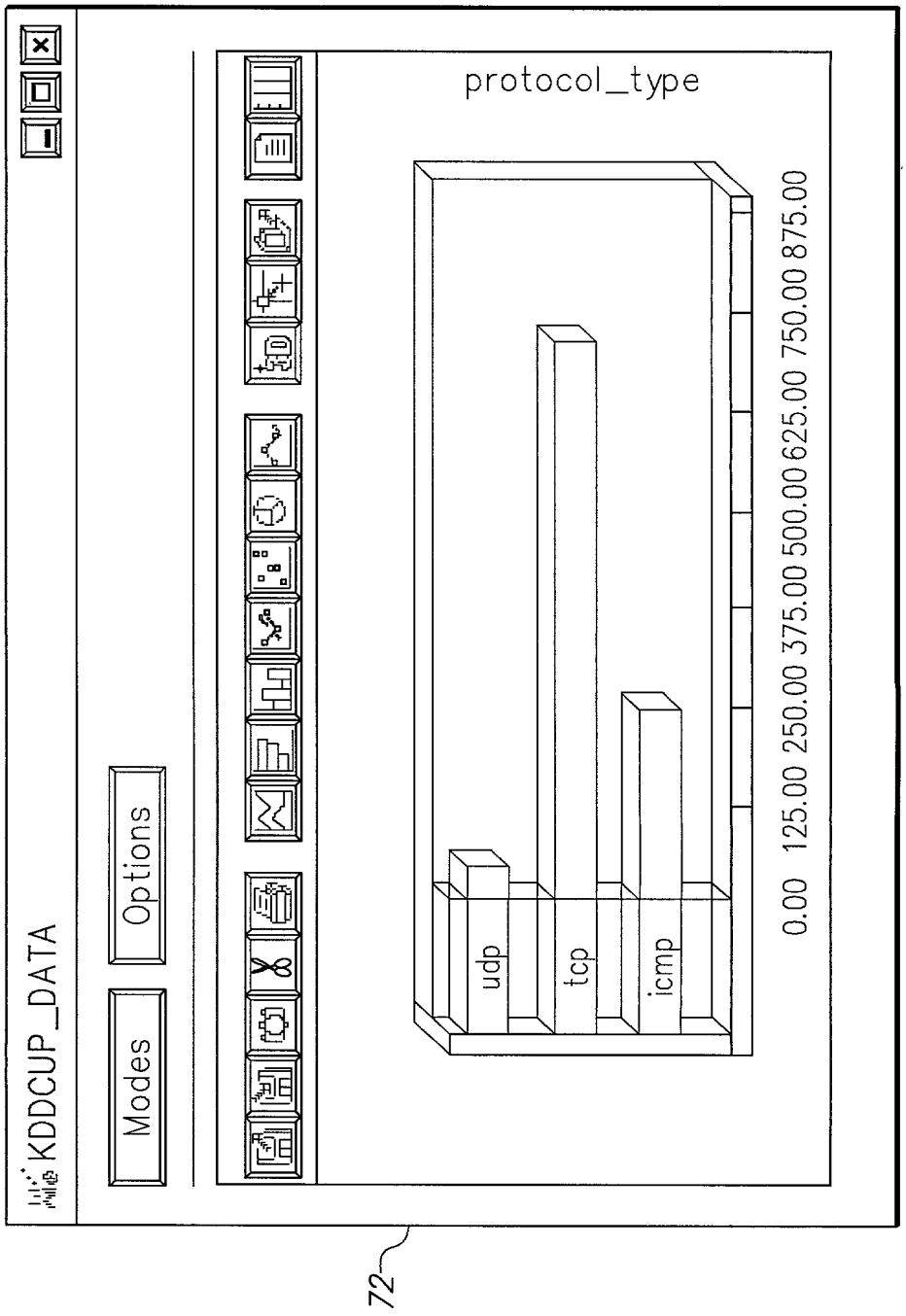

KDDCUP_DATA
Modes
Options
protocol_type
0.00 125.00 250.00 375.00 500.00 625.00 750.00 875.00
udp
tcp
icmp
72

FIG. 7A

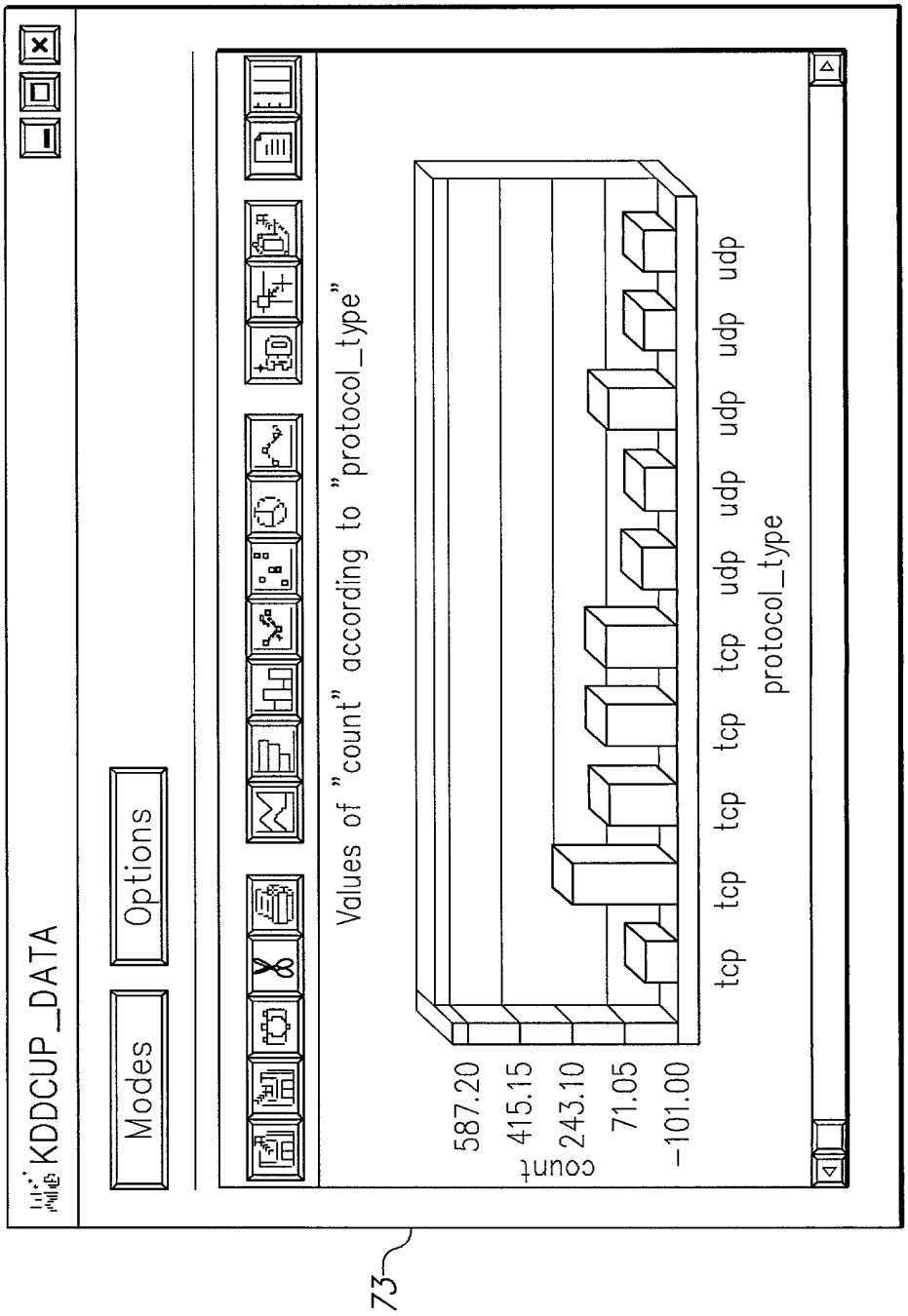

KDDCUP_DATA
Modes
Options
Values of "count" according to "protocol_type"
count
587.20
415.15
243.10
71.05
-101.00
tcp tcp tcp tcp tcp udp udp udp udp udp
protocol_type
73

FIG. 7B

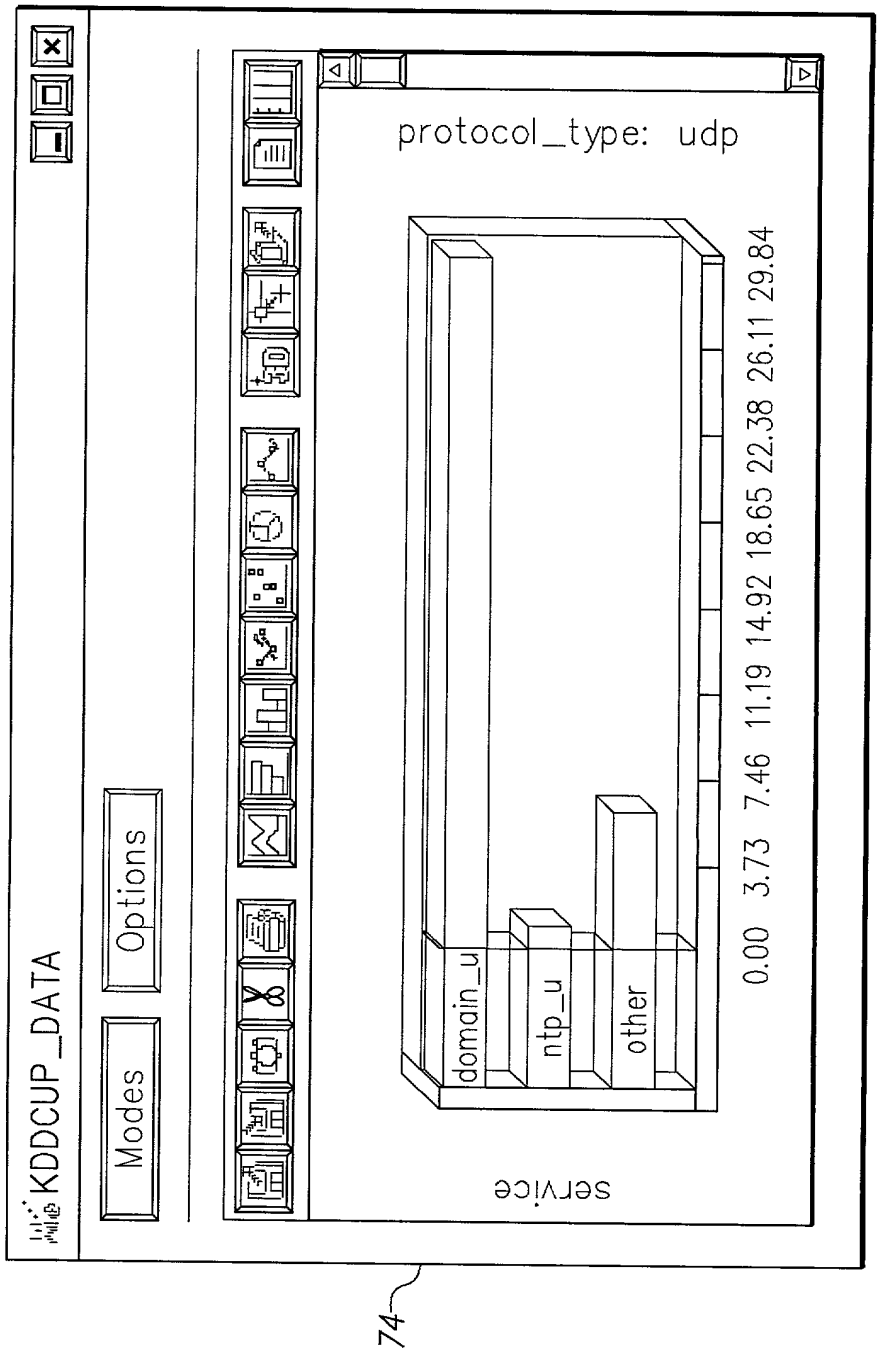

KDDCUP_DATA
Modes
Options
protocol_type: udp
0.00 3.73 7.46 11.19 14.92 18.65 22.38 26.11 29.84
domain_u
ntp_u
other
service
74

FIG. 7C

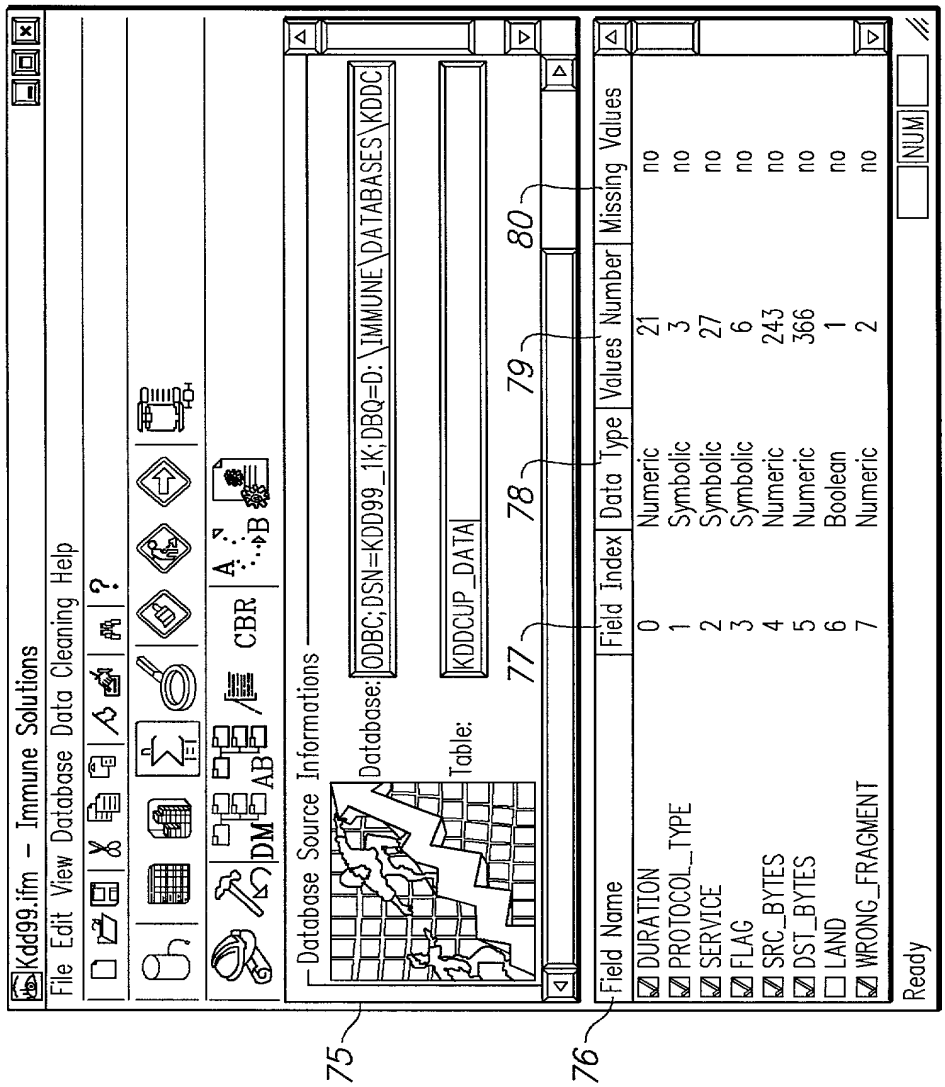

Kdd99.ifm – Immune Solutions
File Edit View Database Data Cleaning Help
Database Source Informations
Database: ODBC;DSN=KDD99_1K;DBQ=D:\IMMUNE\DATABASES\KDDC
Table: KDDCUP_DATA
Field Name | Field Index | Data Type | Values Number | Missing Values
DURATION 0 Numeric 21 no
PROTOCOL_TYPE 1 Symbolic 3 no
SERVICE 2 Symbolic 27 no
FLAG 3 Symbolic 6 no
SRC_BYTES 4 Numeric 243 no
DST_BYTES 5 Numeric 366 no
LAND 6 Boolean 1 no
WRONG_FRAGMENT 7 Numeric 2 no
Ready
NUM
75
76
77
78
79
80

FIG. 8

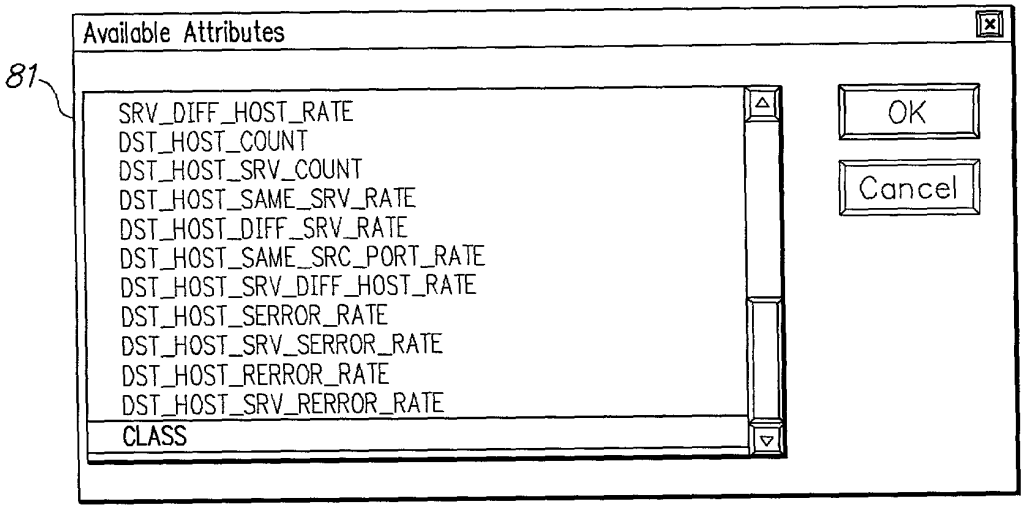

Available Attributes
81
SRV_DIFF_HOST_RATE
DST_HOST_COUNT
DST_HOST_SRV_COUNT
DST_HOST_SAME_SRV_RATE
DST_HOST_DIFF_SRV_RATE
DST_HOST_SAME_SRC_PORT_RATE
DST_HOST_SRV_DIFF_HOST_RATE
DST_HOST_SERROR_RATE
DST_HOST_SRV_SERROR_RATE
DST_HOST_RERROR_RATE
DST_HOST_SRV_RERROR_RATE
CLASS
OK
Cancel

FIG. 9

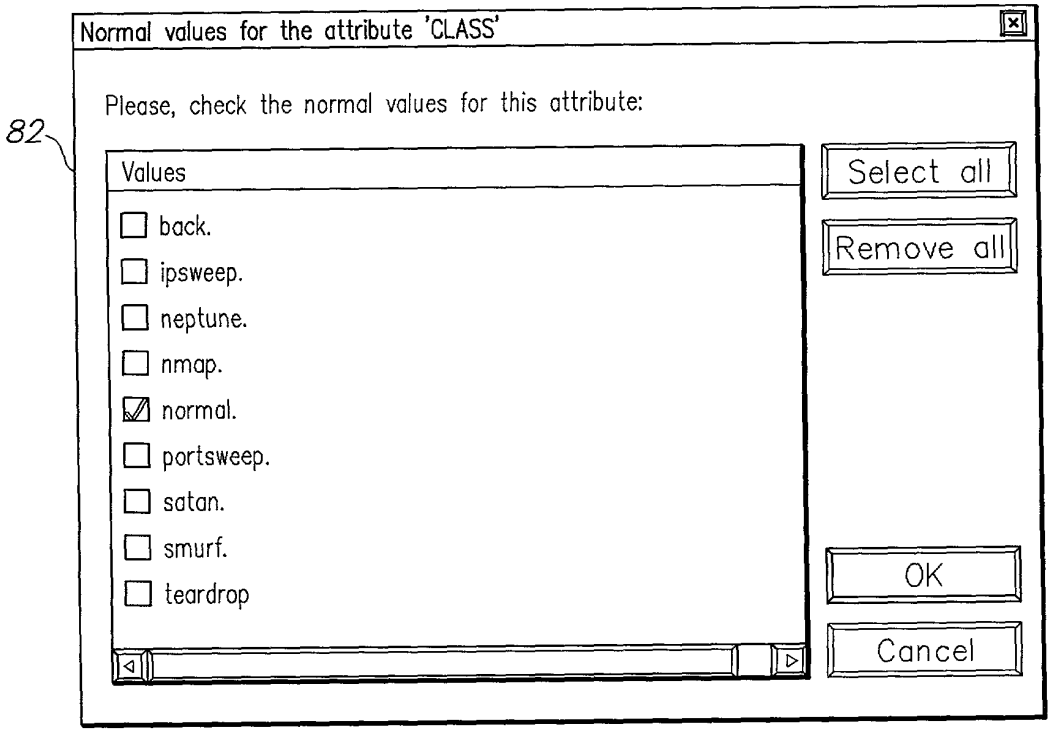

Normal values for the attribute 'CLASS'
Please, check the normal values for this attribute:
82
Values
back.
ipsweep.
neptune.
nmap.
normal.
portsweep.
satan.
smurf.
teardrop
Select all
Remove all
OK
Cancel

FIG. 10

FIG. 11

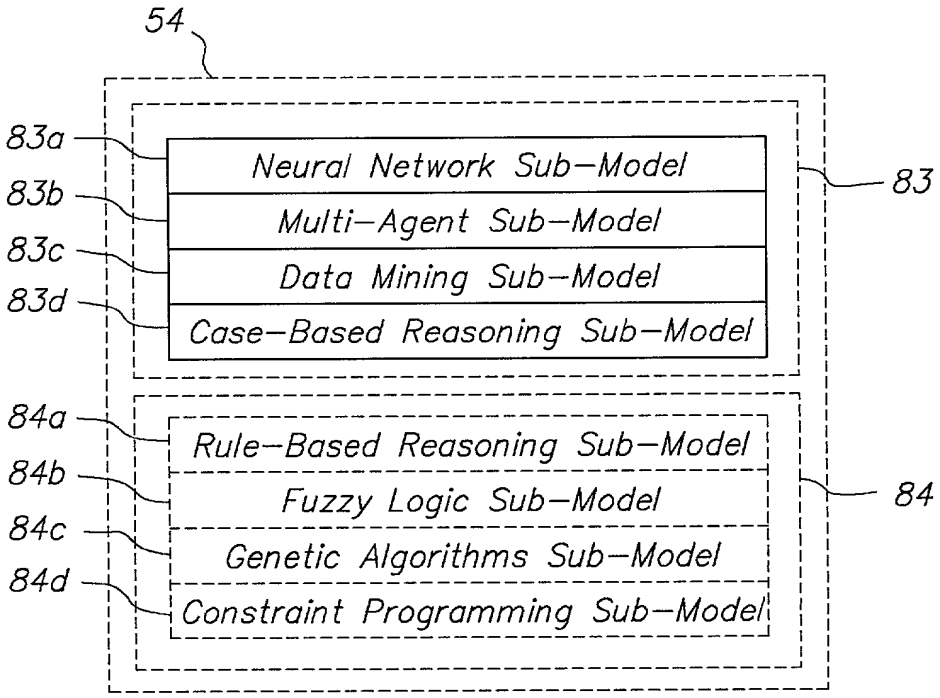

54
83a
83b
83c
83d
Neural Network Sub-Model
Multi-Agent Sub-Model
Data Mining Sub-Model
Case-Based Reasoning Sub-Model
83
84a
84b
84c
84d
Rule-Based Reasoning Sub-Model
Fuzzy Logic Sub-Model
Genetic Algorithms Sub-Model
Constraint Programming Sub-Model
84

FIG. 12

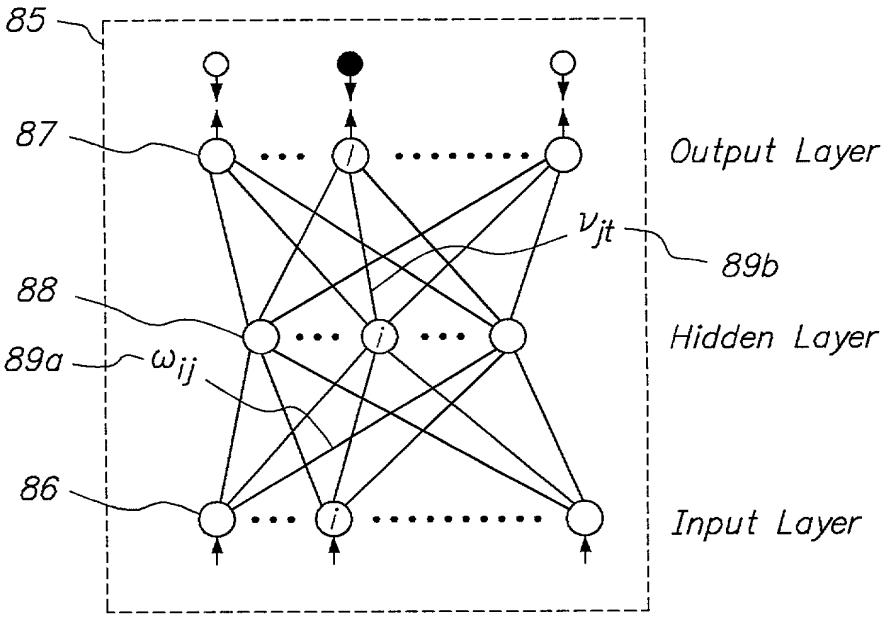

85
87
Output Layer
v_{jt}
89b
88
Hidden Layer
89a
ω_{ij}
86
Input Layer

FIG. 13

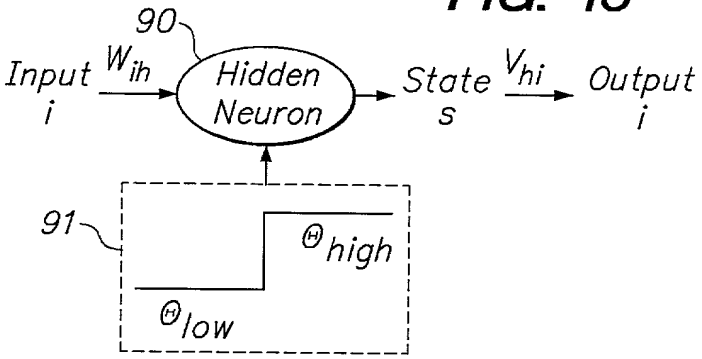
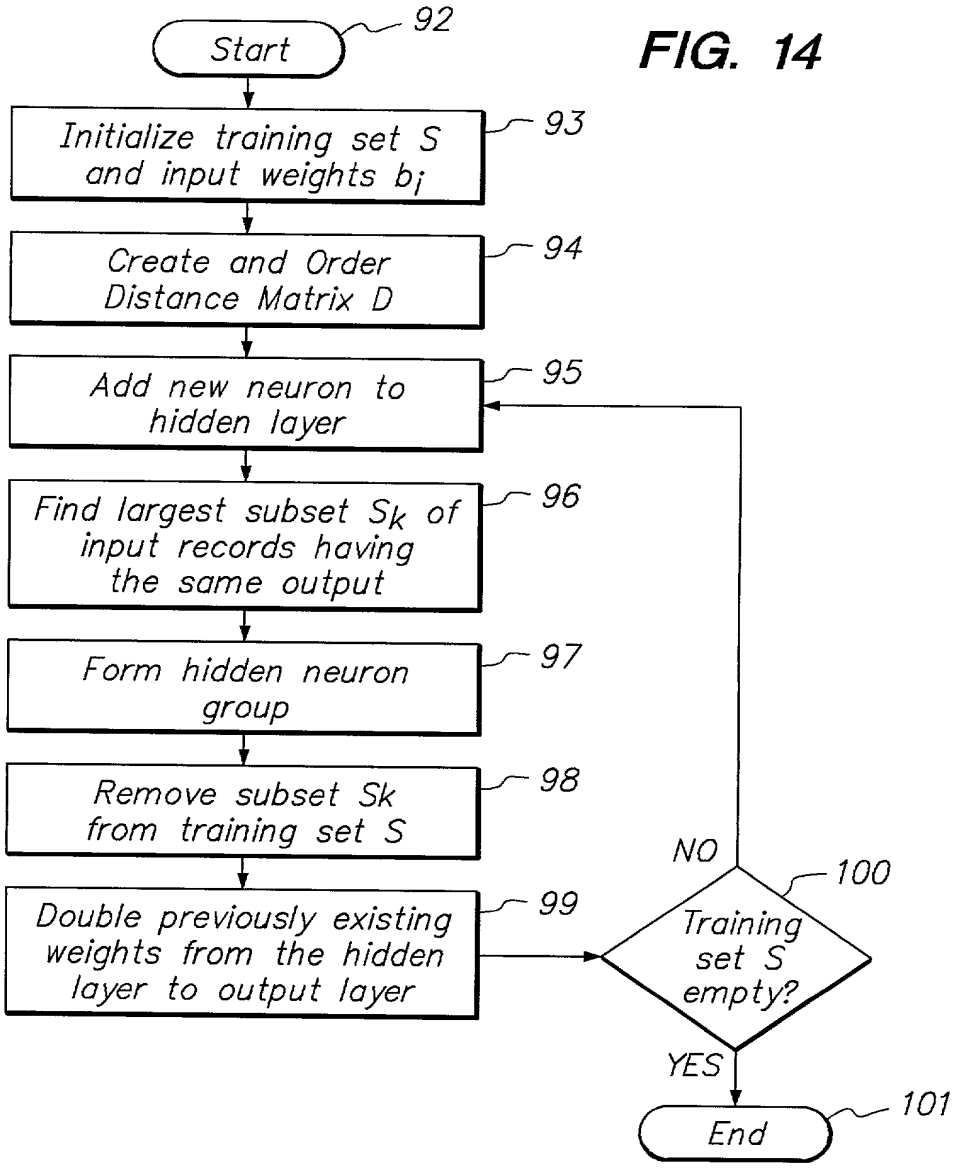

90
Input i
W_{ih}
Hidden Neuron
State s
V_{hi}
Output i
91
Θ_{high}
Θ_{low}

FIG. 14


92
Start
Initialize training set S and input weights b_j
93
Create and Order Distance Matrix D
94
Add new neuron to hidden layer
95
Find largest subset S_k of input records having the same output
96
Form hidden neuron group
97
Remove subset Sk from training set S
98
Double previously existing weights from the hidden layer to output layer
99
NO
Training set S empty?
100
YES
End
101

Applicant : Akli Adjaoute IMN-002
Application No.: 09/810,313 Filed: March 15, 2001
For : SYSTEMS AND METHODS FOR DYNAMIC DETECTION AND PREVENTION OF ELECTRONIC FRAUD AND NETWORK INTRUSION

102

102a	Euclidean	$d(X_i, X_j) = \sqrt{\sum_{k=1}^{M} (X_{i,k} - X_{j,k})^2}$
102b	Manhattan	$d(X_i, X_j) = \sum_{k=1}^{M} \lvert X_{i,k} - X_{j,k} \rvert$
102c	Normalized Euclidean	$d(X_i, X_j) = \sqrt{\frac{1}{M} \sum_{k=1}^{M} \left(\frac{X_{i,k} - X_{j,k}}{max_k - min_k} \right)^2}$
102d	Normalized Manhattan	$d(X_i, X_j) = \frac{1}{M} \sum_{k=1}^{M} \left\lvert \frac{X_{i,k} - X_{j,k}}{max_k - min_k} \right\rvert$
102e	Weighted–Euclidean	$d(X_i, X_j) = \sqrt{\sum_{k=1}^{M} b_i * (X_{i,k} - X_{j,k})^2}$

FIG. 15

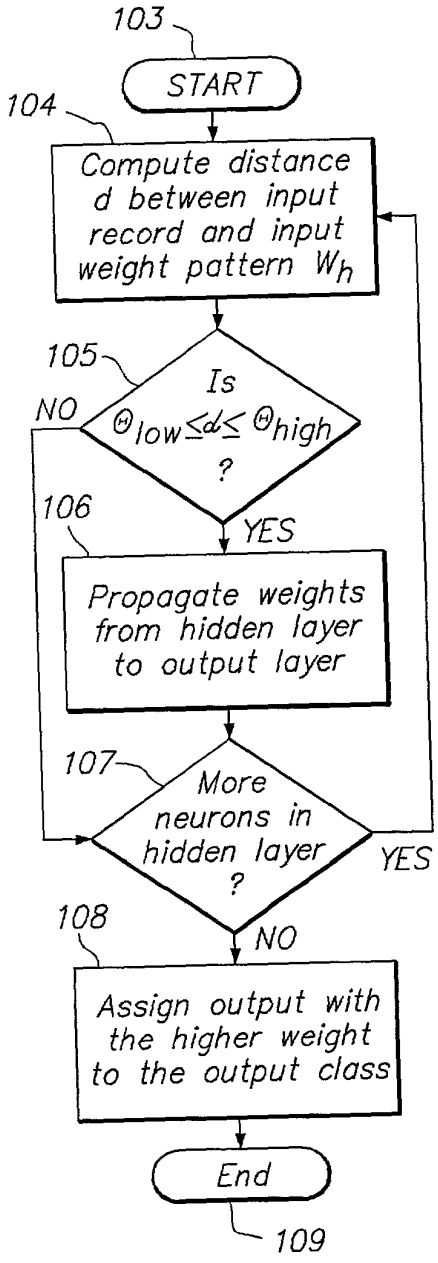


FIG. 16

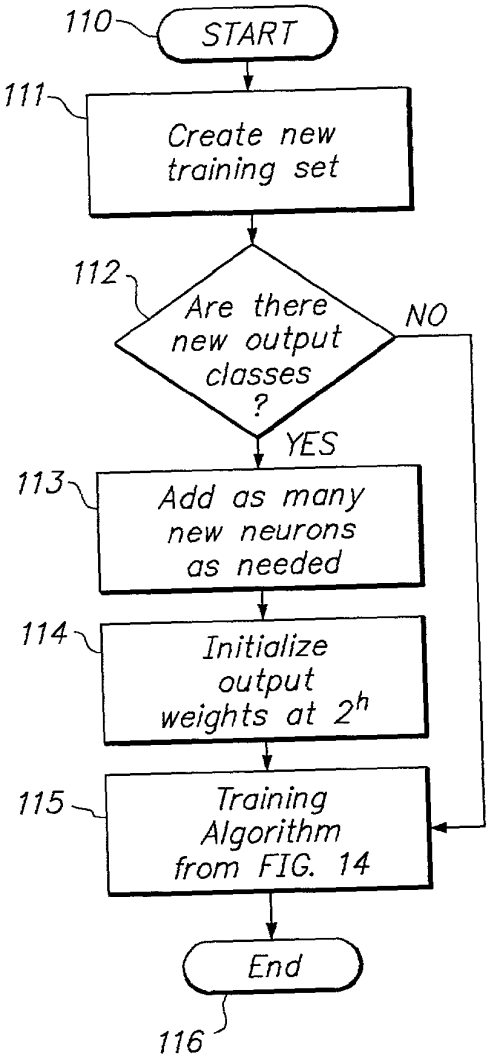
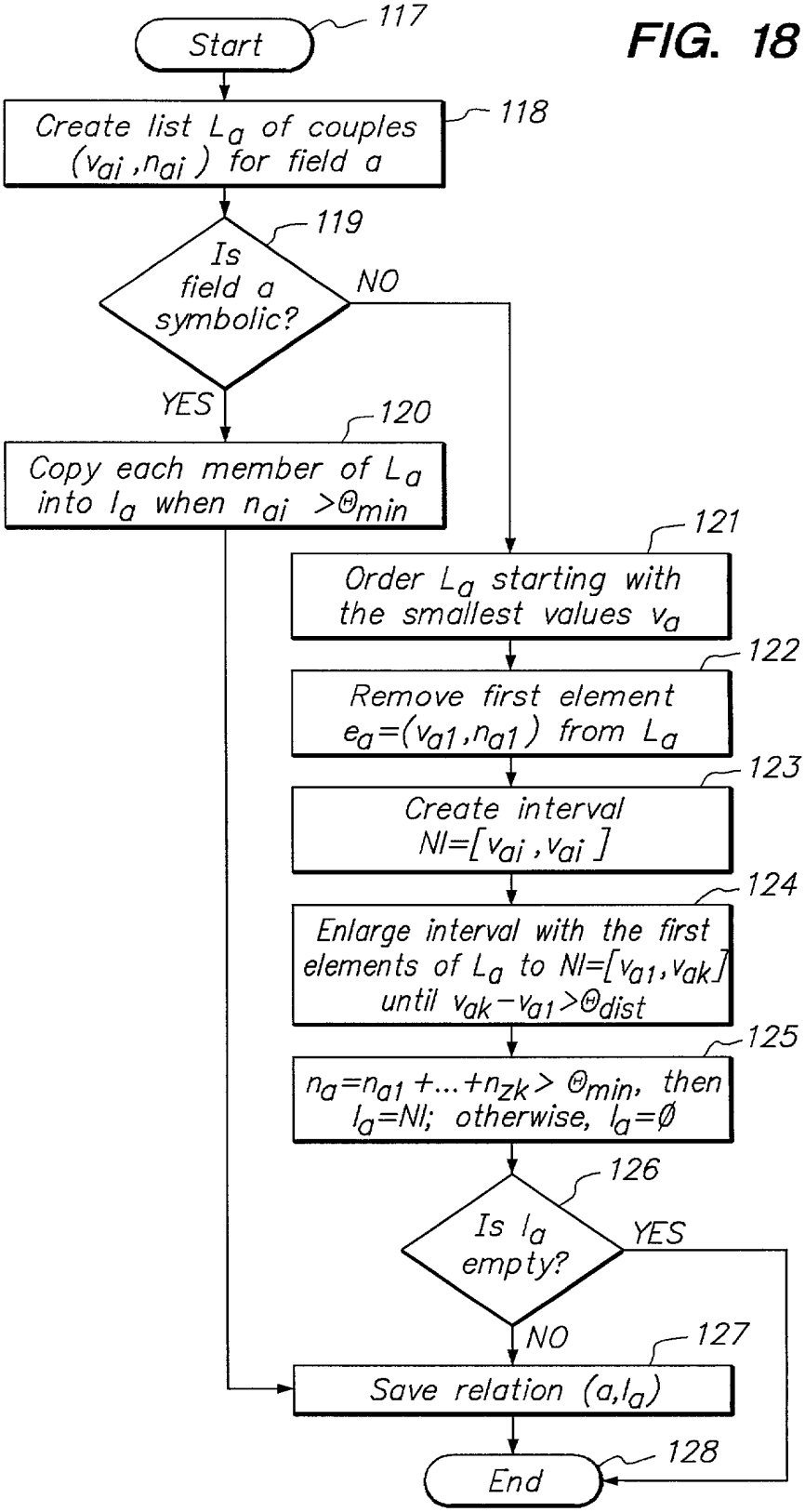


FIG. 17

FIG. 18


Start
117
Create list L_a of couples (v_{ai}, n_{ai}) for field a
118
Is field a symbolic?
119
NO
YES
Copy each member of L_a into l_a when $n_{ai} > \Theta_{min}$
120
Order L_a starting with the smallest values v_a
121
Remove first element $e_a=(v_{a1}, n_{a1})$ from L_a
122
Create interval $NI=[v_{ai}, v_{ai}]$
123
Enlarge interval with the first elements of L_a to $NI=[v_{a1}, v_{ak}]$ until $v_{ak}-v_{a1}>\Theta_{dist}$
124
$n_a=n_{a1}+...+n_{zk}>\Theta_{min}$, then $l_a=NI$; otherwise, $l_a=\emptyset$
125
Is l_a empty?
126
YES
NO
Save relation (a, l_a)
127
End
128

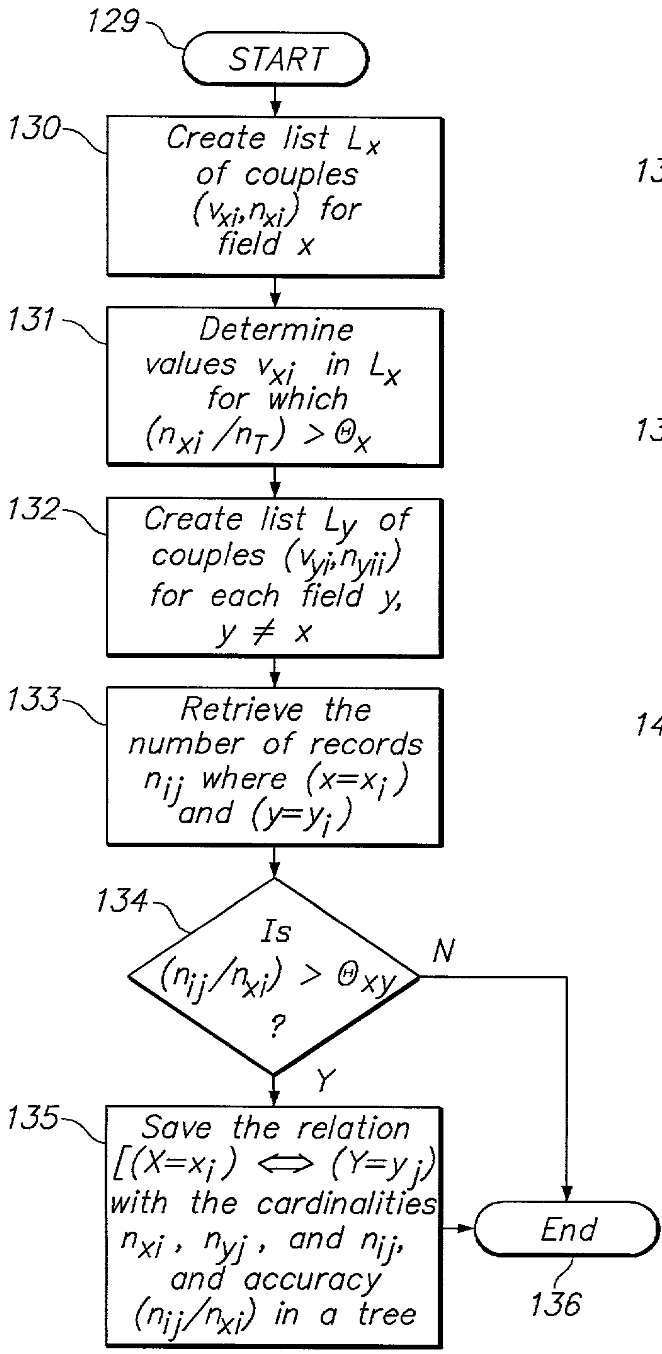

129
START
130
Create list L_x of couples (v_{xi}, n_{xi}) for field x
131
Determine values v_{xi} in L_x for which $(n_{xi}/n_T) > \Theta_x$
132
Create list L_y of couples (v_{yi}, n_{yii}) for each field y, $y \neq x$
133
Retrieve the number of records n_{ij} where $(x=x_i)$ and $(y=y_i)$
134
Is $(n_{ij}/n_{xi}) > \Theta_{xy}$?
N
Y
135
Save the relation $[(X=x_i) \Leftrightarrow (Y=y_j)]$ with the cardinalities n_{xi}, n_{yj}, and n_{ij}, and accuracy (n_{ij}/n_{xi}) in a tree
End
136

FIG. 19

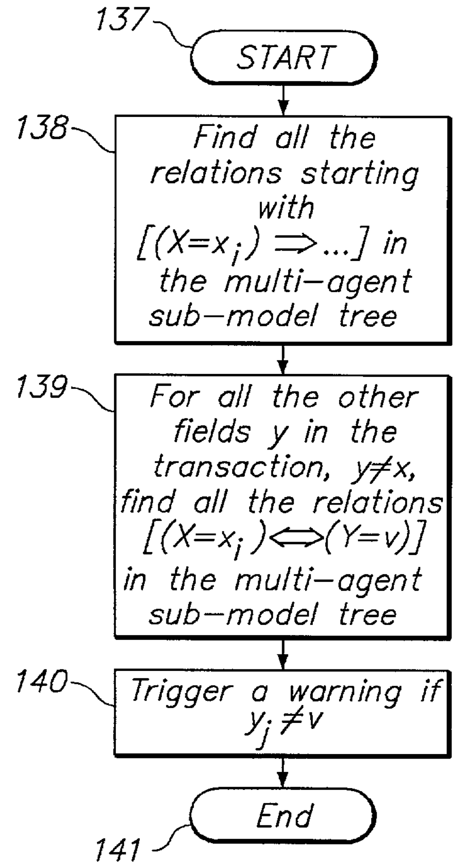

137
START
138
Find all the relations starting with $[(X=x_i) \Rightarrow ...]$ in the multi-agent sub-model tree
139
For all the other fields y in the transaction, $y \neq x$, find all the relations $[(X=x_i) \Leftrightarrow (Y=v)]$ in the multi-agent sub-model tree
140
Trigger a warning if $y_j \neq v$
End
141

FIG. 20

FIG. 21

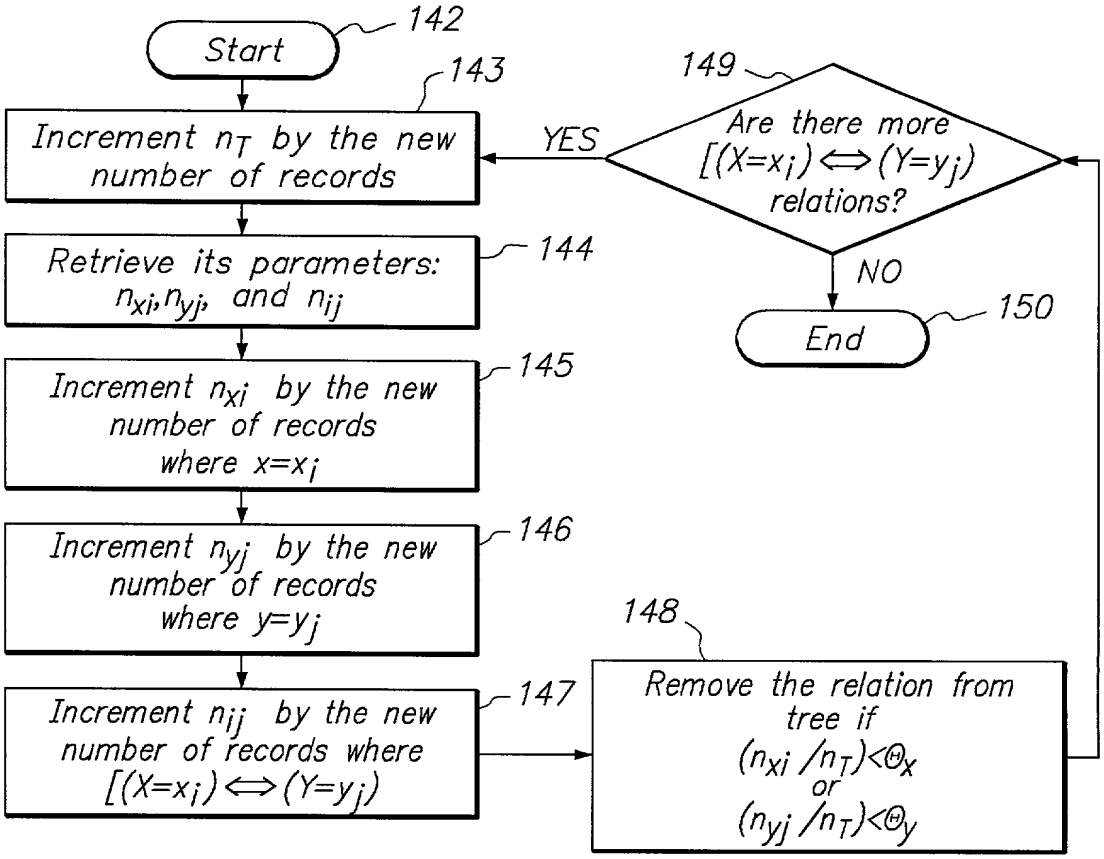
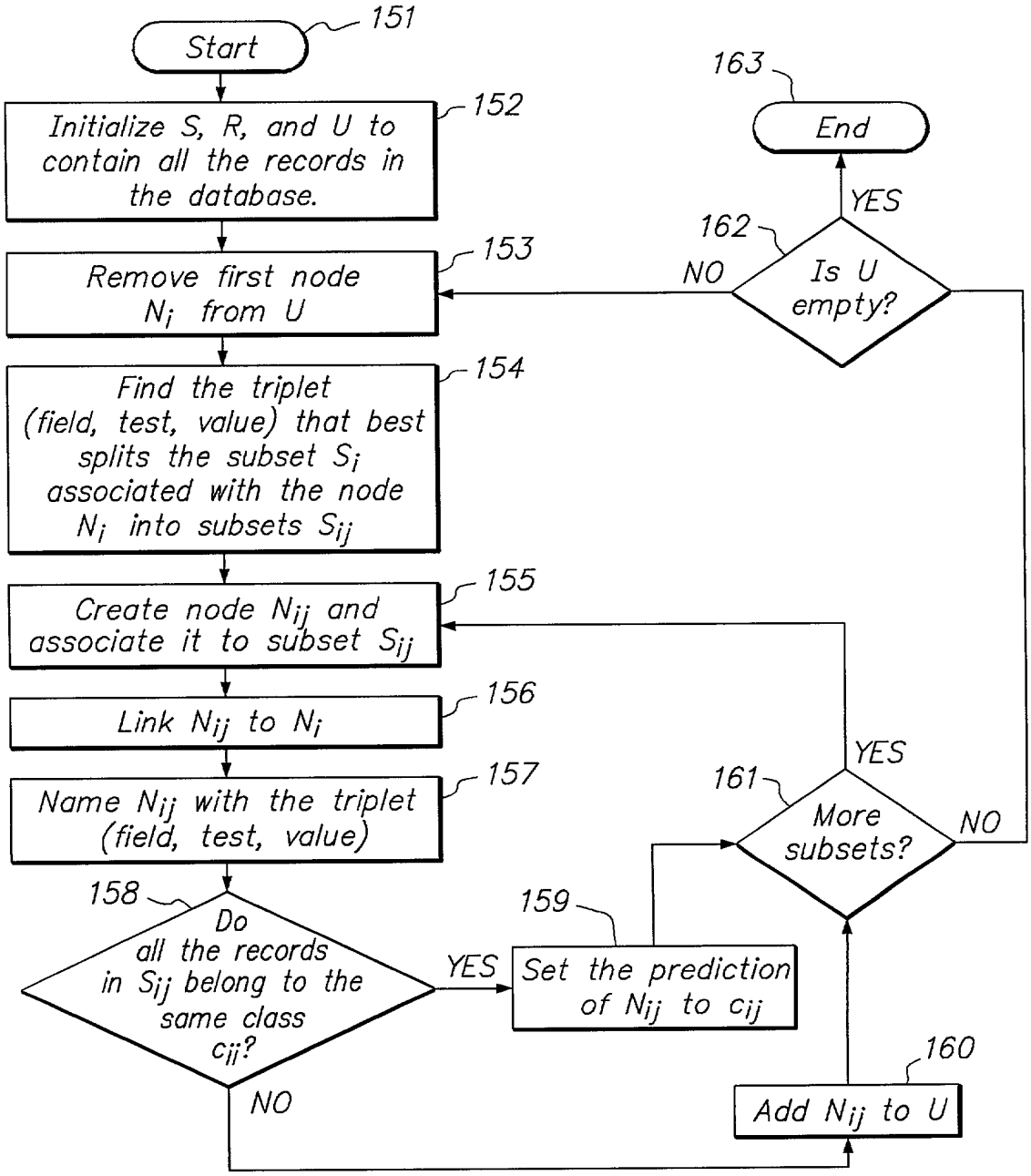


FIG. 22


Start
151
Initialize S, R, and U to contain all the records in the database.
152
Remove first node N_i from U
153
Find the triplet (field, test, value) that best splits the subset S_i associated with the node N_i into subsets S_{ij}
154
Create node N_{ij} and associate it to subset S_{ij}
155
Link N_{ij} to N_i
156
Name N_{ij} with the triplet (field, test, value)
157
Do all the records in S_{ij} belong to the same class c_{ij}?
158
YES
Set the prediction of N_{ij} to c_{ij}
159
NO
Add N_{ij} to U
160
More subsets?
161
YES
NO
Is U empty?
162
YES
NO
End
163

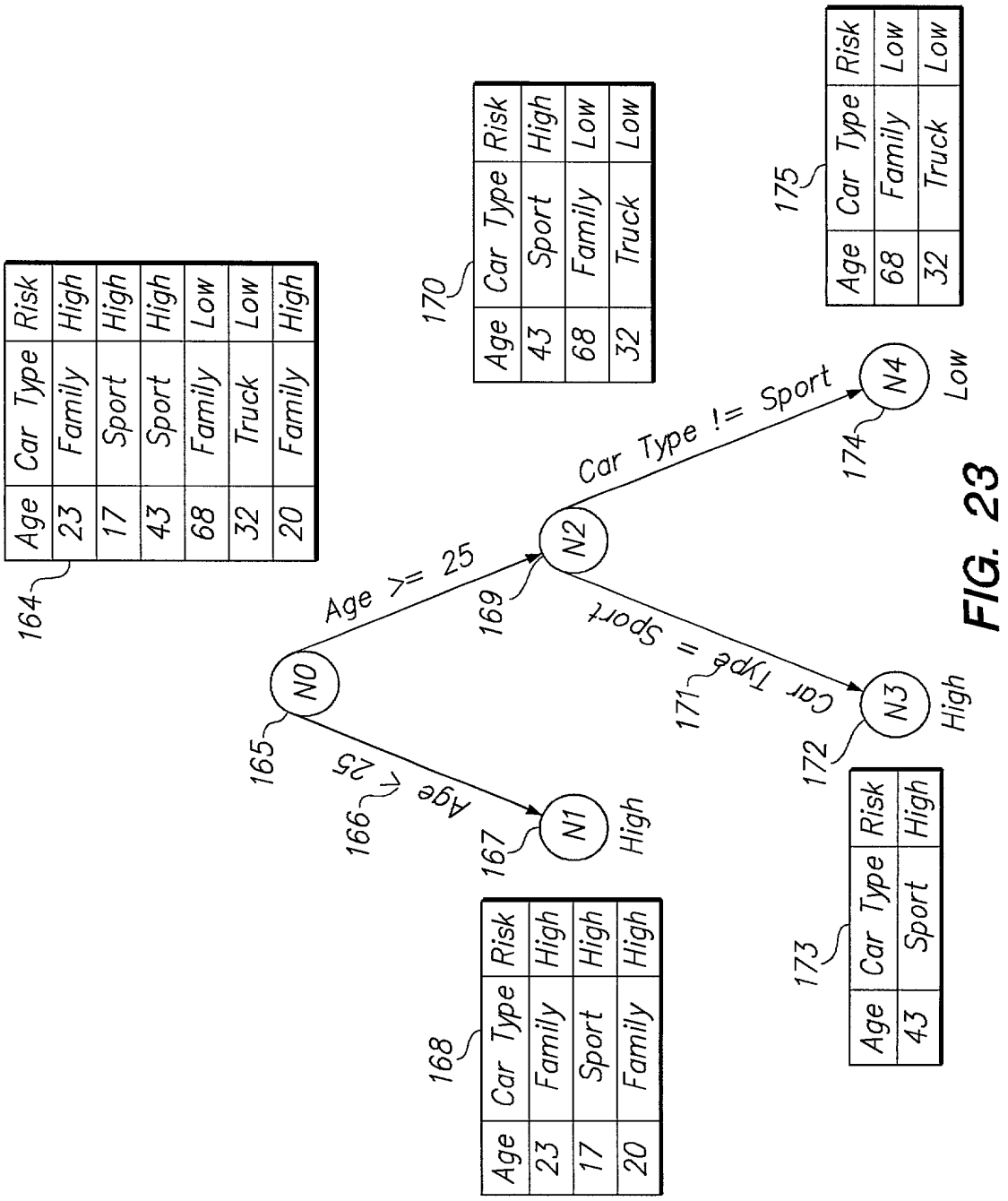

N0
N1
N2
N3
N4
Age >= 25
Age < 25
Car Type != Sport
Car Type = Sport
High
Low
164
165
166
167
168
169
170
171
172
173
174
175
Age | Car Type | Risk
23 | Family | High
17 | Sport | High
43 | Sport | High
68 | Family | Low
32 | Truck | Low
20 | Family | High
Age | Car Type | Risk
43 | Sport | High
68 | Family | Low
32 | Truck | Low
Age | Car Type | Risk
23 | Family | High
17 | Sport | High
20 | Family | High
Age | Car Type | Risk
43 | Sport | High
Age | Car Type | Risk
68 | Family | Low
32 | Truck | Low

FIG. 23

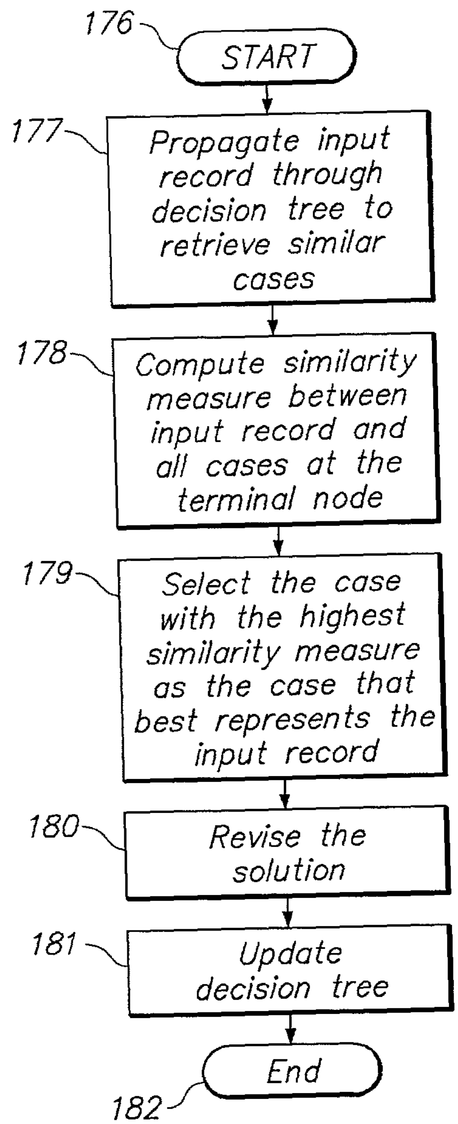

176
START
177
Propagate input record through decision tree to retrieve similar cases
178
Compute similarity measure between input record and all cases at the terminal node
179
Select the case with the highest similarity measure as the case that best represents the input record
180
Revise the solution
181
Update decision tree
End
182

FIG. 24

Applicant : Akli Adjaoute IMN-002
Application No.: 09/810,313 Filed: March 15, 2001
For : SYSTEMS AND METHODS FOR DYNAMIC DETECTION AND PREVENTION OF ELECTRONIC FRAUD AND NETWORK INTRUSION

183

Global Similarity Measure	Expression
City-block	$\frac{1}{\rho}\sum_{i=4}^{\rho} sim_i(V_{1i}, V_{2i})$
Weighted city-block	$\frac{1}{\rho}\sum_{i=4}^{\rho} w_i * sim_i(V_{1i}, V_{2i})$
Euclidean	$\frac{1}{\rho}\sqrt{\sum_{i=4}^{\rho} sim_i(V_{1i}, V_{2i})^2}$
Minkowski	$\frac{1}{\rho}\sqrt[r]{\sum_{i=1}^{\rho} sim_i(V_{1i}, V_{2i})^r}$
Weighted Minkowski	$\sqrt[r]{\sum_{i=1}^{\rho} w_i * sim_i(V_{1i}, V_{2i})^r}$
Weighted maximum	$max_i \; w_i * sim_i(V_{1i}, V_{2i})$

FIG. 25

184

Local Similarity Measures	Field Type	Field Valuation
$\begin{cases} 0, & \text{if } V_1 \cap V_2 = \emptyset \\ 1, & \text{otherwise} \end{cases}$	Nominal	Single, multiple
$\frac{Card(V_1 \cup V_2) - Card(V_1 \cap V_2)}{Card(V_1 \cup V_2)}$	Nominal	Multiple
$\frac{Card(V_1 \cup V_2) - Card(V_1 \cap V_2)}{Min(V_1 \cup V_2)}$	Nominal	Multiple
$\frac{Card(V_1 \cup V_2) - Card(V_1 \cap V_2)}{Max(V_1 \cup V_2)}$	Nominal	Multiple
$\frac{Card(V_1 \cup V_2) - Card(V_1 \cap V_2)}{Card(0)}$	Nominal	Multiple
$\frac{ec(min(V_1^-, V_2^-), max(V_1^+, V_2^+)) - Card(V_1 \cap V_2)}{Card(0)}$	Ordinal, Numeric	Multiple
$\frac{\lvert V_1 - V_2 \rvert}{ec(0)}$	Numeric	Single
$\frac{\lvert V_{1c} - V_{2c} \rvert}{ec(0)}$	Numeric	Multiple
$\frac{ec(min(V_1^-, V_2^-), max(V_1^+, V_2^+)) - ec(V_1 \cap V_2)}{ec(0)}$	Numeric	Multiple
$\frac{ec(V_1 \cup V_2) - ec(V_1 \cap V_2)}{ec(V_1 \cup V_2)}$	Numeric	Multiple
$\frac{ec(V_1 \cup V_2) - ec(V_1 \cap V_2)}{min(ecV_1, ecV_2)}$	Numeric	Multiple
$\frac{ec(V_1 \cup V_2) - ec(V_1 \cap V_2)}{max(ecV_1, ecV_2)}$	Numeric	Multiple
$\frac{2 * h(V_1 \cup V_2) - h(V_1) - h(V_2)}{2 * h_{max}}$	Taxonomic	Multiple
$\frac{h(\text{node that unit } V_1 \ \& \ V_2)}{\text{total height of } h}$	Taxonomic	Single

FIG. 26

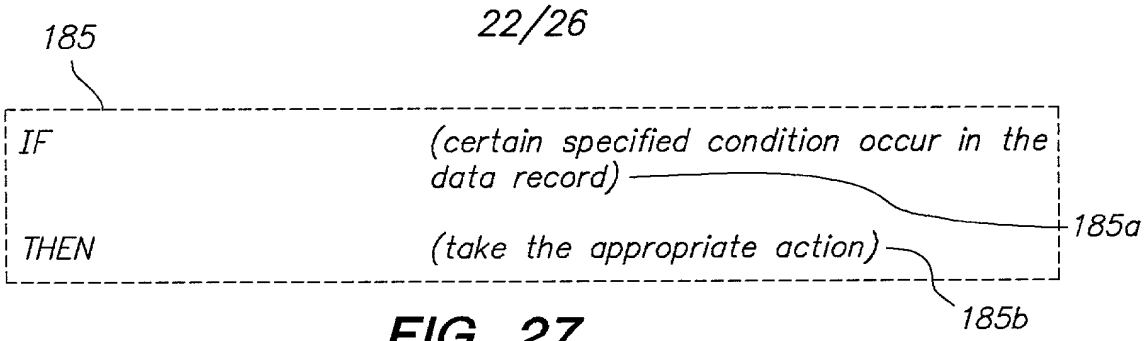


FIG. 27

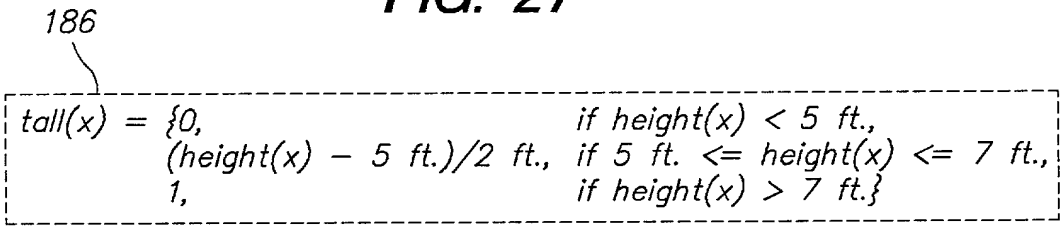


FIG. 28

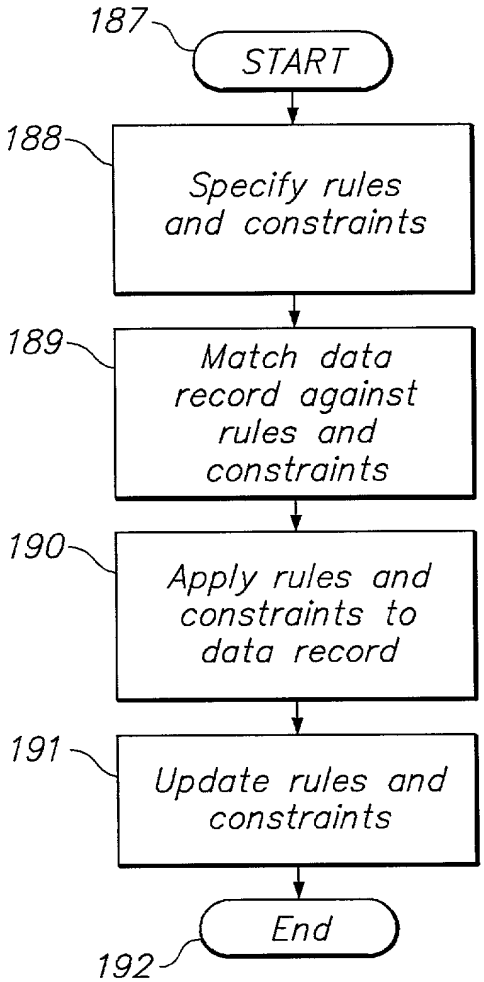


FIG. 29

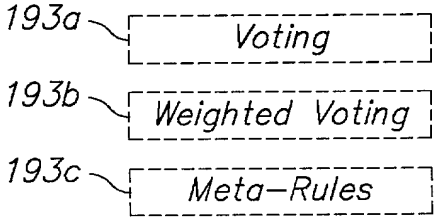


FIG. 30

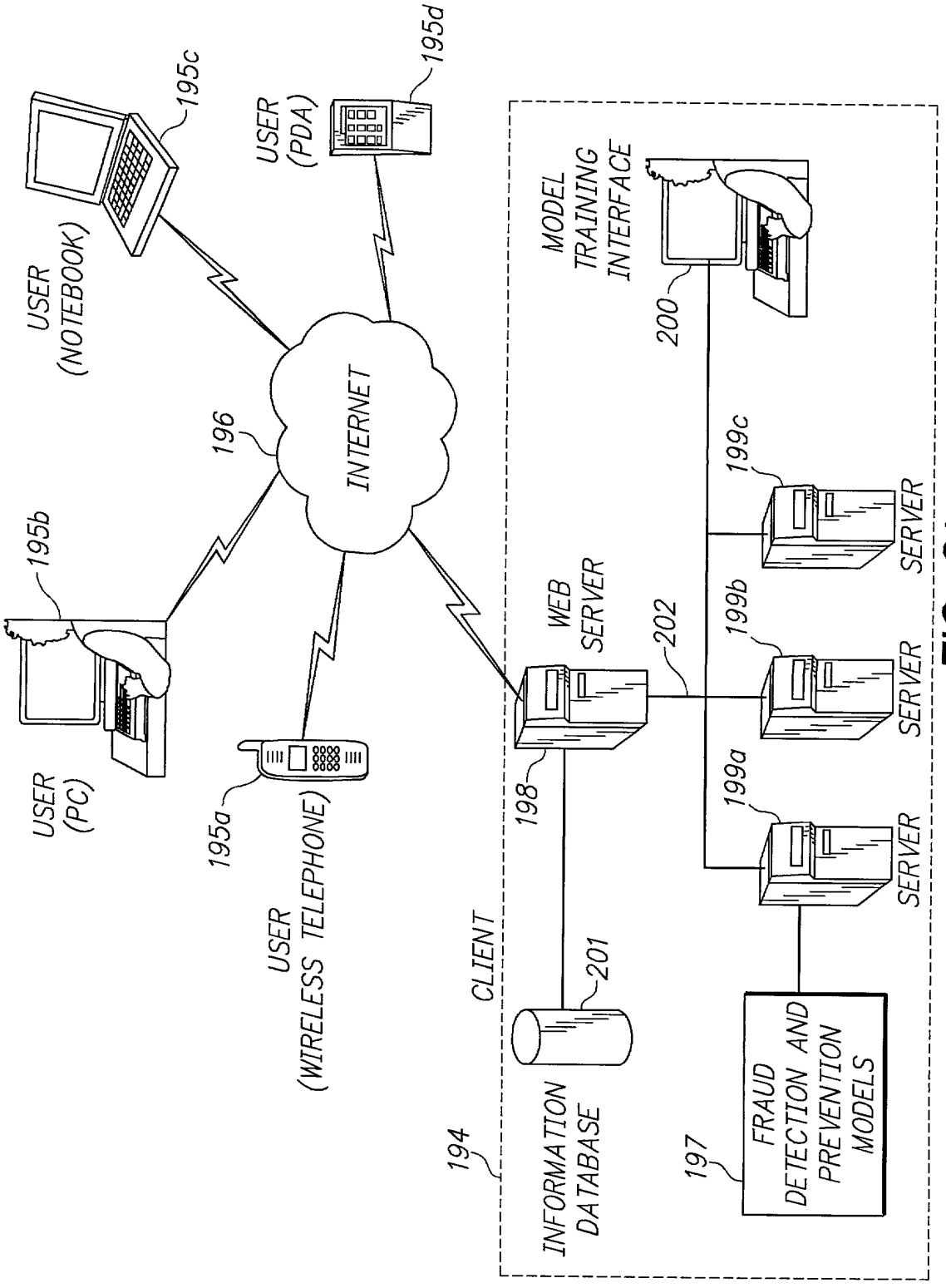

USER (NOTEBOOK)
195c
USER (PDA)
195d
INTERNET
196
USER (PC)
195b
USER (WIRELESS TELEPHONE)
195a
MODEL TRAINING INTERFACE
200
WEB SERVER
202
198
SERVER
199c
SERVER
199b
SERVER
199a
CLIENT
201
INFORMATION DATABASE
194
FRAUD DETECTION AND PREVENTION MODELS
197

FIG. 31

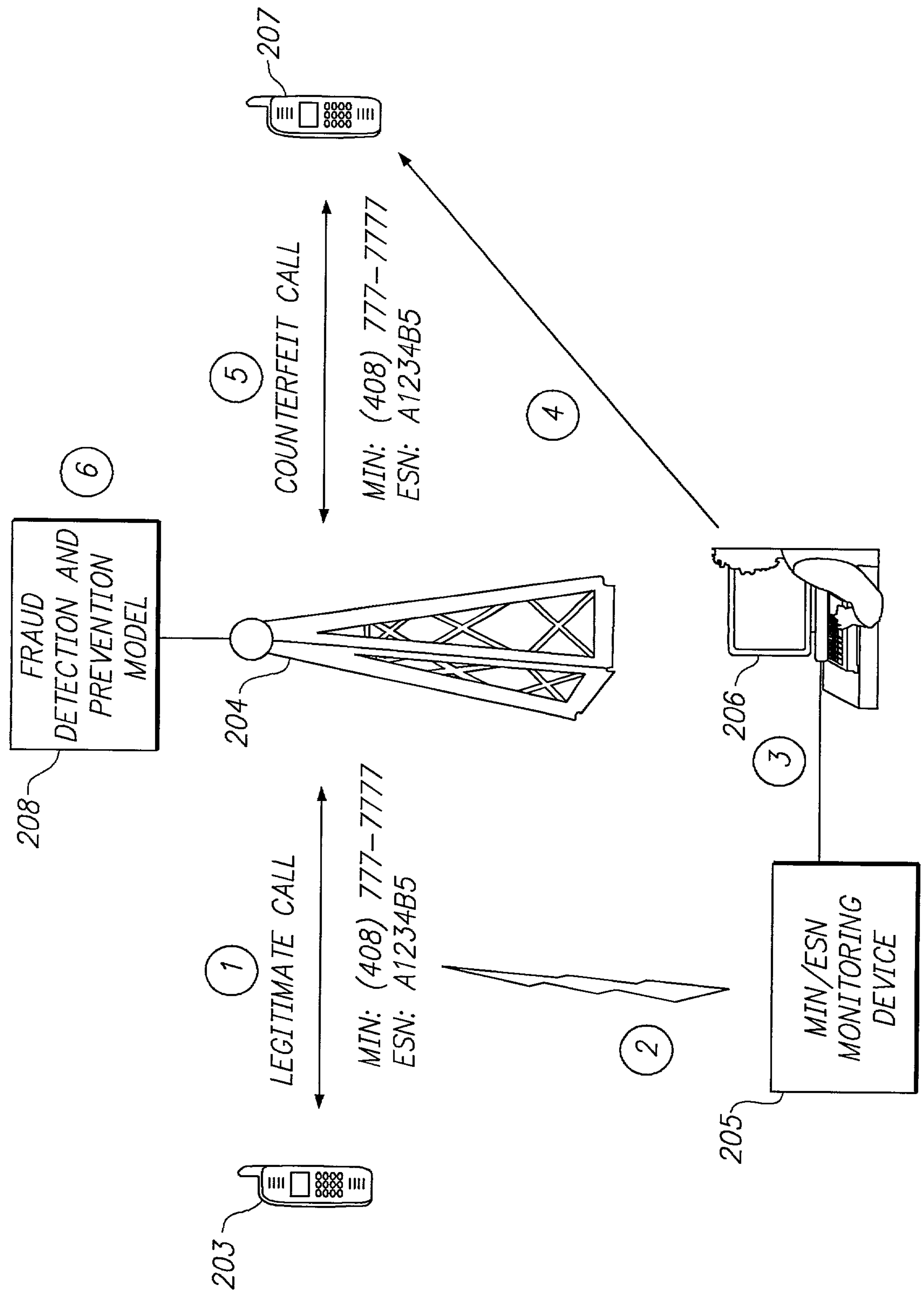

207
5
COUNTERFEIT CALL
MIN: (408) 777-7777
ESN: A1234B5
6
4
FRAUD DETECTION AND PREVENTION MODEL
208
204
206
3
1
LEGITIMATE CALL
MIN: (408) 777-7777
ESN: A1234B5
2
MIN/ESN MONITORING DEVICE
205
203

FIG. 32

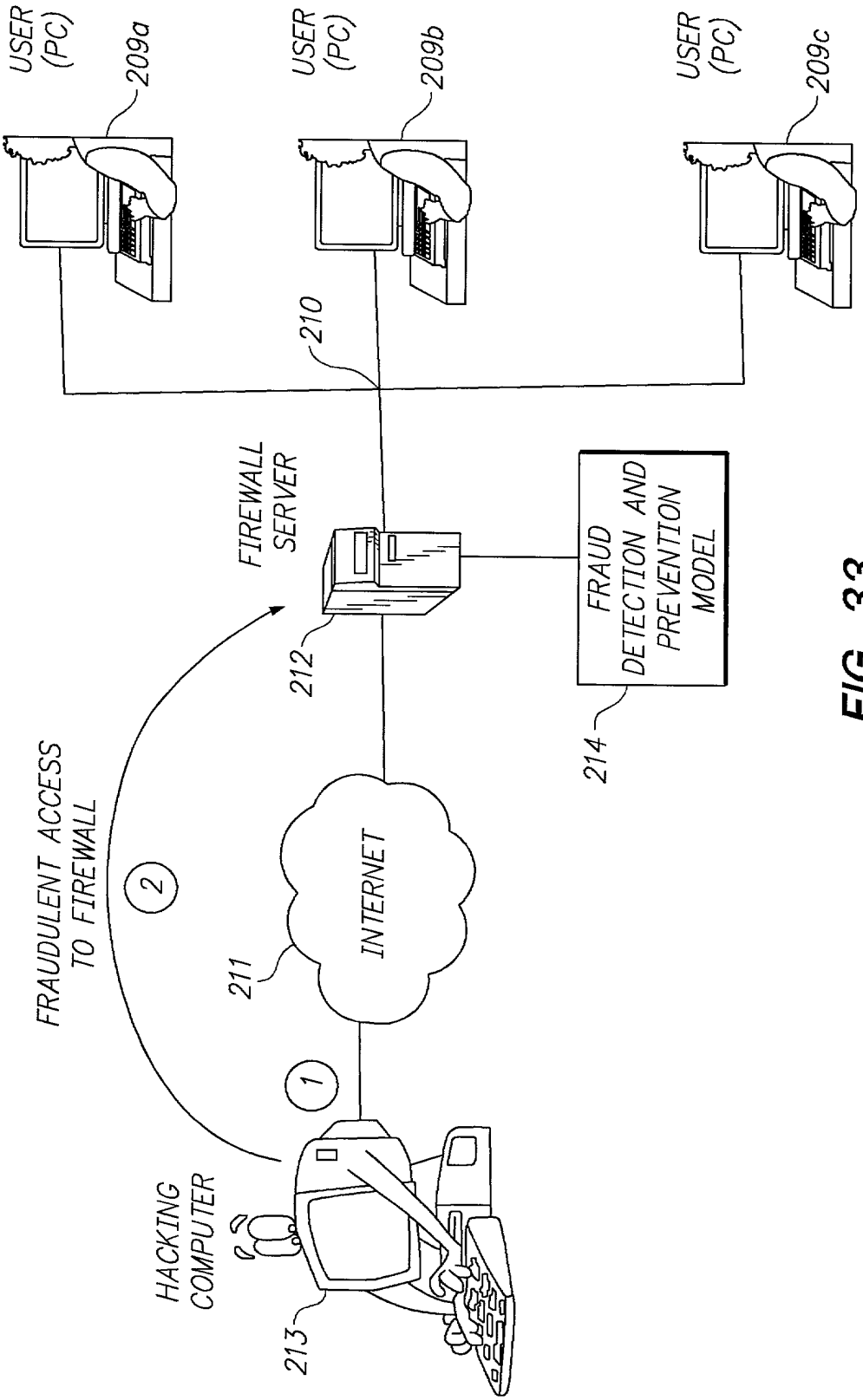

USER (PC)
209a
USER (PC)
209b
USER (PC)
209c
210
FIREWALL SERVER
212
FRAUD DETECTION AND PREVENTION MODEL
214
INTERNET
211
FRAUDULENT ACCESS TO FIREWALL
2
1
HACKING COMPUTER
213

FIG. 33

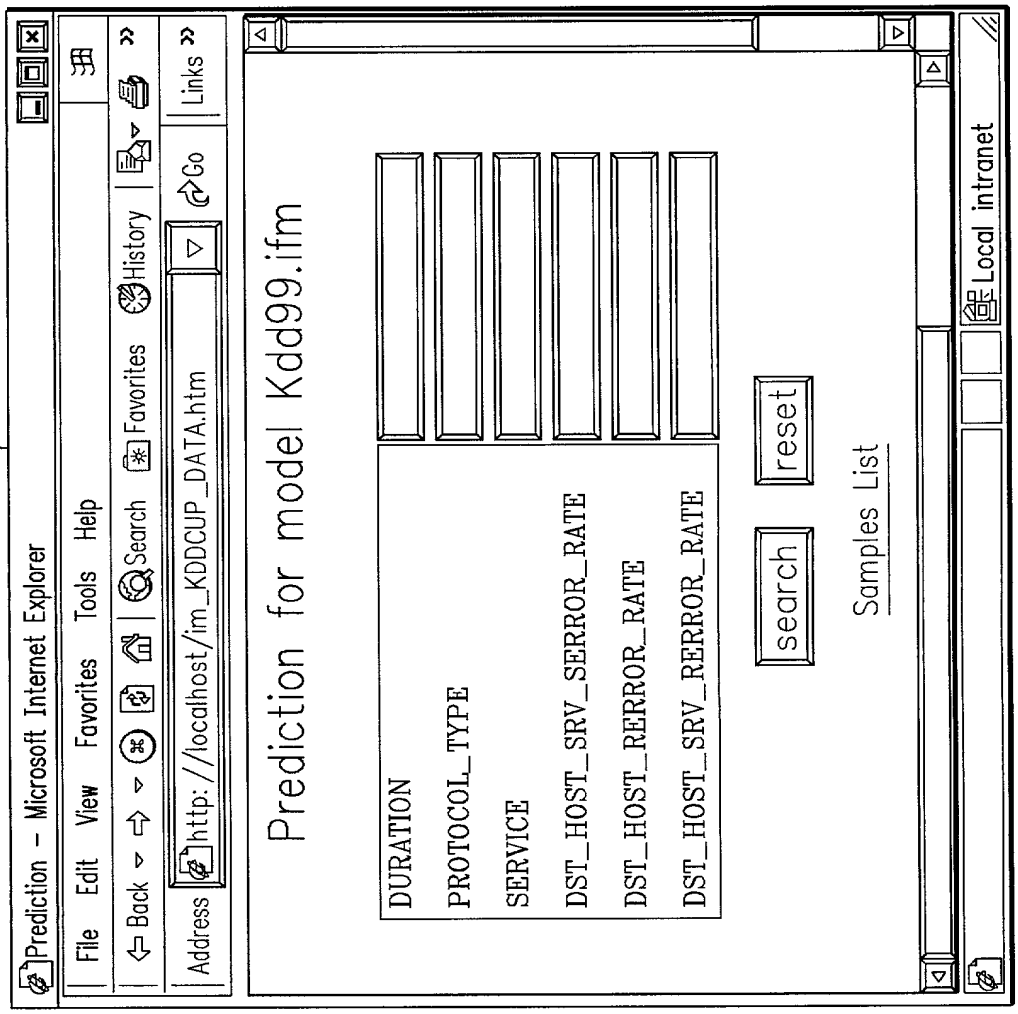

215
Prediction - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://localhost/im_KDDCUP_DATA.htm
Go
Links
Prediction for model Kdd99.ifm
DURATION
PROTOCOL_TYPE
SERVICE
DST_HOST_SRV_SERROR_RATE
DST_HOST_RERROR_RATE
DST_HOST_SRV_RERROR_RATE
search
reset
Samples List
Local intranet

FIG. 34